

SECURITY REQUIREMENTS

ECF

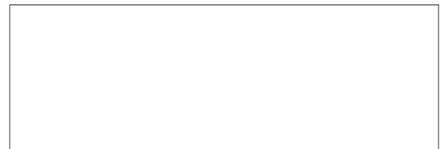
AUTOMATED INFORMATION SYSTEMS

ICCATFI

IN OVERSEAS INSTALLATIONS

SECRET

- 1 -



25X1

SECRET

TABIE CF CCNTEENTS

SECTION

I Purpose

II Applicability

III Responsibilities

- A. Headquarters Component
- B. Overseas Location
- C. Information Systems Security Group (ISSG), Office of Security
- D. Overseas Security Support Branch (CSSB), Office of Security
- E. Communications Security Division (CSD), Office of Communications
- F. Area Headquarters, Office of Communications
- G. Technical Security Division (TSD), Office of Security

IV System Security Requirements

A. Physical Security

- 1. ADF Facility Location
- 2. User Terminal Locations
- 3. ADF Facility Construction Criteria
- 4. Personnel Access Controls
 - a. Station or Base
 - b. ADF Facility
 - c. Storage Areas
- 5. Data and Program Storage Media
 - a. Identification/Labeling
 - b. Storage
 - c. Open Shelf Storage
 - d. Transportation
 - e. Logging and Personal Accountability

E. Technical Security

- 1. Audic Countermeasures
- 2. Alarm Systems
- 3. Procedures - Alarm Activation
- 4. Procedures - Alarm Failure

C. Communications Security

- 1. Equipment Installation
 - a. General

SECRET

- b. Power
- c. Conduit
- 2. Telecommunications Equipment Installation
 - a. Standards
- 3. Telecommunications Signal Lines
 - a. Criteria
- 4. Emanations
- 5. Cryptographic Security

D. Information Systems Security

- 1. Systems Hardware
- 2. System Software
- 3. Data Files
- 4. Sanitization/Destruction
 - a. Policy
 - b. Procedures
- 5. System Access Controls
 - a. Remote Terminals/Terminal Areas
- 6. Audit Trails

V System Operation

- A. System Preparation
- E. Data Processing
- C. Processing Termination - Normal
- E. Processing Termination - Emergencies

VI System Equipment Transportation and Storage

- A. Transportation
- E. Storage

VII System Maintenance/Modifications

- A. System Hardware
- E. System Software

VIII Emergency Procedures

APPENDIXES

SECRET

I Purpose

This manual establishes security requirements, standards, and specifications for the protection of word and/or data processing (ADP) systems (hereinafter referred to as automated information processing systems) and information stored in or processed by [] information systems located in overseas Stations or Bases (hereinafter referred to as "overseas location(s)").

25X1

II Applicability

The security requirements, standards, and specifications established herein apply to all automated information processing systems used at overseas locations. This includes systems which interface with telecommunications services, as well as stand-alone, interactive, and networked systems. These requirements do not replace or supersede existing minimum security requirements established by other directives, but rather establish a base for additional security requirements.

III Responsibilities

A. Responsible Headquarters Component

The Headquarters Component having primary responsibility for the proposed site of an automated information processing system in an overseas location shall:

1. Request of the Chief, Information Systems Security Group (ISSG), Office of Security, the necessary pre-installation security survey of the proposed overseas location.
2. In coordination with the Chief of Station or Base, approve the designation of a station/base assigned individual to act as the ADE System Security Officer for the proposed automated information processing system and related equipment.
3. In coordination with the Chief of Station or Base, the assigned Information System Security Officer (ISSC), and other Headquarters components as required, develop an ADE System Installation [] tailored to the selected Station or Base environment. (See Paragraph C. below)
4. Submit the developed ADE System Installation Plan to the Chief, ISSG, Office of Security, for final approval. The transmittal document will include a certification that the requirements, standards, and specifications recommended by the pre-installation security survey team, and established herein, are to

ILLEGIB

SECRET

be implemented for the Station or Base.

5. In coordination with the designated Information Systems Security Officer (ISSO), develop Station or Base Emergency Plan documentation for the evacuation and/or destruction of data and program storage media, and system equipment.

B. Overseas Location

The Chief of each Station or Base proposing to use an automated information processing system shall:

1. Provide area, space, and any special recommendations to the appropriate Headquarters component for inclusion in the ADF System Installation Plan.
2. In coordination with the Headquarters component, designate a station/base assigned individual to act as the ADF System Security Officer. The designation of an alternate ADF System Security Officer is recommended.
3. Direct the ADF System Security Officer to establish and implement, in coordination with the designated Information Systems Security Officer (ISSO), a formal ADF System Security Program to ensure compliance with the requirements established herein for the location's automated information processing system.

C. Information Systems Security Group (ISSG), Office of Security

The Chief, ISSG, (as the [] ISSO) is responsible to determine, formulate, interpret, and disseminate policies; and guide the implementation of the security requirements, standards, and specifications within [] and its facilities to ensure compliance with applicable Executive Orders and Directives relating to information systems, in accordance with ECIE 1/16.

The Chief, ISSG, shall appoint an Information Systems Security Officer (ISSO) for each overseas location designated to use an automated information processing system. The ISSO shall:

1. Serve as the security focal point for each assigned automated information processing system.
2. Review the ADF System Installation Plan for each assigned overseas location to ensure that all requirements, standards, and specifications relevant

~~SECRET~~

to the proposed installation are implemented. This includes obtaining written certification from the responsible Headquarters component of the satisfactory compliance with these requirements.

3. Submit for approval by the Chief, ISSG, the ADP System Installation Plan established for each assigned overseas location.
4. Obtain approval from the Chief, ISSG, for the ADP System Security Program for each assigned overseas location. This program shall include the complete spectrum of security controls and safeguards for each system in each location. The ADP System Security Program shall be prepared with appropriate input from other Headquarters components having specific areas of interest. These include but are not limited to the responsible Headquarters component, the Overseas Security Support Branch (Office of Security), the Communications Security Division (Office of Communications), and the Technical Security Division (Office of Security).
5. Review and recommend approval of pre-installation security surveys of each assigned overseas automated information processing site.
6. Coordinate reports received concerning each assigned overseas location's automated information processing system with the Overseas Security Support Branch (Office of Security), the Communications Security Division (Office of Communications), the Technical Security Division (Office of Security), the responsible Headquarters component, and the appropriate Area Headquarters (Office of Communications).
7. Review the ADP System Security Program implemented for each assigned overseas location for continued compliance with the requirements, standards, and specifications established herein.
8. Schedule an annual security survey and audit of each assigned overseas automated information processing system.

D. Overseas Security Support Branch
(CSSB), Office of Security

The overseas Security Support Branch shall:

1. Interpret, and disseminate policies relating to physical security matters as they pertain to

~~SECRET~~

automated information processing systems in overseas locations.

2. Conduct periodic (minimum once every 2 years) physical security surveys of all [redacted] automated information processing systems in overseas locations. 25X1
3. Coordinate all physical security reports received concerning overseas automated information processing locations with the Information Systems Security Group (Office of Security), the Communications Security Division (Office of Communications), the Technical Security Division (Office of Security), and the responsible Headquarters component.
4. Participate in pre-installation security surveys of proposed overseas automated information processing system locations.

E. Communications Security Division (CSI), Office of Communications

1. Interpret and disseminate policies relating to communications security matters as they pertain to [redacted] automated information processing systems located in overseas locations, including those systems used for telecommunications services. Additionally, [redacted] will retain primary responsibility for the security of any [redacted] automated information processing systems located within [redacted] facilities overseas. 25X1
2. Conduct TEMPEST testing for all [redacted] ALE Systems installed in overseas locations. 25X1
3. Coordinate reports received concerning overseas automated information processing system communications security matters with the Information Systems Security Group (Office of Security), the Overseas Security Support Branch (Office of Security), the Technical Security Division (Office of Security) and the responsible Headquarters component.

F. Area Headquarters, Office of Communications

The Area Headquarters shall:

1. Conduct communications security inspections and COMSEC audits, excluding TEMPEST testing, of all [redacted] automated information processing systems installed in overseas locations. 25X1

SECRET

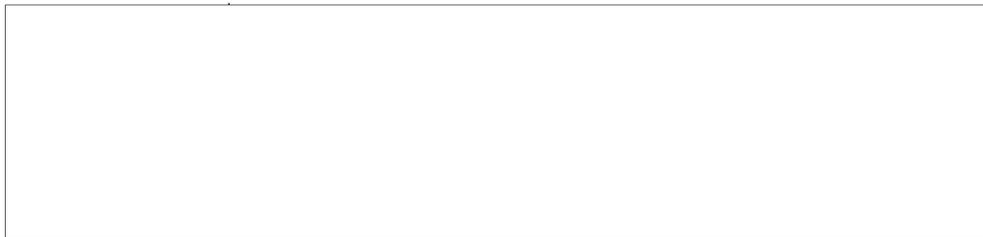
2. Participate in pre-installation security surveys of proposed overseas automated information processing systems.

G. Technical Security Division (TSD),
Office of Security

The Technical Security Division shall:

1. Conduct an Audic Countermeasures (ACM) inspection of all automated information processing system locations, and all user terminal positions remote from the automated information processing system central processor.
2. Install an approved alarm system in the ADF Facility and all areas remote from the AIP Facility in which user terminals are positioned. ("ADF Facility" is defined in Section IV A).
3. Conduct Periodic Audic Countermeasures (ACM) reinspections:

- a.
- b.
- c.



25X1

IV System Security Requirements

A. Physical Security

1. ADP Facility Location

All central processors and equipment units directly associated therewith shall be located within controlled space within the overseas location, in an interior room, when possible, and on a floor which precludes access from the outside (hereinafter referred to as the "ADF Facility").

25X1

2. User Terminal Locations

All user terminals should be located within the ADF Facility. Recognizing, however, that Station or Base operational requirements or physical restrictions may preclude the installation of all user terminals within the ADF Facility, the following requirements are established as minimum for the location of user terminals in positions remote from the ADF Facility:

SECRET

~~SECRET~~

a. All user terminals shall be located within [] controlled space. 25X1

b. All user terminals shall be located in alarm protected areas and, when possible, in rooms meeting the criteria for a "secure area". (See Section IV E-Technical Security and Section IV C-Communications Security).

3. ADP Facility Construction Criteria

a. Existing Buildings

An ADP Facility which is to be located in an existing building shall be constructed to meet the existing criteria for a "secure area".

b. New Buildings

ADP Facilities which are planned for installation in new buildings []

[] shall be located in a secure area within the [] controlled portion of the building. The selected location shall provide for the maximum security of the planned automated information processing equipment as well as the associated data and program storage media, and shall meet the existing criteria for designation as a "Secure Area". Additionally, ADP facilities which are planned to contain cryptographic hardware or materials shall adhere to []

[] Standards for construction and be approved by the Office of Communications.

4. Personnel Access Controls

a. Station or Base

Approved 24 hour a day [] guard protection is required at each location in which an ADP Facility is installed. Headquarters will normally not approve installation of an ADP Facility in overseas locations lacking the 24 hour approved [] guard because of the inability to provide satisfactory alarm response.

b. ADP Facility

Only [] Staff employees who possess an established need-to-know, as determined by the Chief of Station or Base, shall be allowed access

~~SECRET~~

SECRET

to the ADF Facility. If cryptographic equipment or material is installed in the ADF Facility, appropriate Cryptographic clearances are required. (See Section IV Paragraph (4b)).

c. Storage Areas

Only [] staff employees who possess an established need-to-know shall be allowed access to the approved storage area in which data and program storage media are maintained.

25X1

5. Data and Program Storage Media

a. Identification/Labeling

- 1) Demountable data and program storage media (magnetic tapes, disk packs, floppy disks, and cassettes) shall bear an external label to clearly indicate the highest security classification and/or compartments of the information stored on the media.
- 2) Card decks shall be marked so as to clearly indicate the highest security classification and/or compartments of the information stored on the deck.
- 3) Program listings and all hardcopy output, including program listings and hardcopy output on microfilm, shall be labeled so as to clearly indicate the highest security classification and/or compartments of the information listed or printed.
- 4) Any punched paper tapes used shall be labeled and marked so as to clearly indicate the highest security classification and/or compartments of the information recorded.

b. Storage

All demountable data and program storage media, when not being used, shall be placed in an approved Class 5 security container. These security containers may be located within the ADF Facility or the Station/ Base vault or secure area provided the Station/ Base vault or secure area meets the standards established for an ADF Facility.

c. Open Shelf Storage

Facilities planning to use ADF systems possessing

SECRET

~~SECRET~~

fixed storage media or internal memory units which are non-volatile, shall only be approved when the construction of the ADF Facility meets the requirements for open shelf storage of the material to be stored, and a formal waiver is granted. See Section IV, Paragraph 11.

d. Transportation

The physical movement of all demountable data and program storage media outside the approved secure area, or between the overseas location's buildings, shall be accomplished in accordance with existing requirements for the movement of classified documents of an equal classification. The prescribed and approved logging and personal accountability procedures shall be used.

e. Logging and Personal Accountability

- 1) A logging and personal accountability system shall be established and maintained, and shall be based on procedures approved by the designated Information System Security Officer.
- 2) Staff employees shall be designated and identifiable on an access list to receipt for all classified data and program storage media.
- 3) The logging and personal accountability system shall include logs for the removal and return of all demountable data and program storage media from and to the approved storage area.
- 4) The access lists and the logging and personal accountability system shall be periodically reviewed by the designated Information Systems Security Officer to determine their accuracy and currency.

25X1

F. Technical Security

1. Audic Countermeasures

An Audic Countermeasures (PCM) inspection will be conducted in the proposed ADF Facility and in all areas remote from the ADF Facility in which user terminals are to be positioned, prior to the operational implementation of any automated information processing.

2. Alarm Systems

~~SECRET~~

SECRET

The ADF Facility and all areas remote from the ADF Facility in which user terminals are to be positioned shall be equipped with an Office of Security approved alarm system. If the ADF Facility, or any user terminal area, is partitioned into separate areas by wall to ceiling panels, each subdivided area shall have an independent alarm and/or sensor.

3. Procedures - Alarm Activation

a. An alarm activation must be responded to within 5 minutes regardless of the time of day.

b. The [] guard shall immediately summon the responsible [] officer. 25X1
25X1

c. The responsible [] officer shall inspect the alarmed area for evidence of a penetration or attempted entry. 25X1

d. If evidence of a penetration or attempted entry is discovered, the responsible [] officer shall: 25X1

- 1) Secure the affected area. If the ADF Facility or area in which a remote user terminal is located cannot be secured after an alarm activation, the area shall be occupied by a [] staff employee until the alarm system is restored to service. 25X1

(NOTE: If evidence of a penetration or attempted entry is discovered, without an alarm activation, normal Station/Case physical security procedures shall be implemented.)

- 2) Report the incident, via an IMMEDIATE cable slugged [] to the appropriate regional security group, with an INFC copy to Headquarters. Areas not under the jurisdiction of a regional security group shall report the incident to Headquarters. 25X1

(NOTE: If cryptographic equipment is located in the affected area, the cable shall be slugged [] and the appropriate CC Area Headquarters added as an INFC copy recipient.) The cable shall include: 25X1

- a) Time of alarm activation
- b) Area of alarm activation

SECRET

~~SECRET~~

- c) Type of alarm (volumetric or door contact)
- d) Condition at the time of alarm activation, ie.
 - (1) Was there a power failure in the area?
 - (2) Did alarm function properly when checked following the activation?
 - (3) Any other information which will assist Headquarters or the Chief, Regional Security Group, to determine whether the information processing equipment affected can be placed back in operation, and when.
- 3) Maintain the affected area and equipment in a fully secure status until a response is received.
- 4) Following the response, arrange for the conduct of a full audio countermeasures and TEMPEST inspection prior to placing the area and equipment back into service.

4. Procedures - Alarm Failure

In the event of an alarm failure the responsible [redacted] officer shall:

25X1

- a. Report the incident via a PRIORITY cable slugged [redacted] to the appropriate regional security group, with an INFO copy to Headquarters. The cable shall include:

25X1

- 1) Time alarm failure discovered
 - 2) Area of alarm failure
 - 3) Type of alarm (volumetric or door contact)
 - 4) As much information about the alarm failure as possible to assist the regional security group and or Headquarters to diagnose the failure problem. If repair instructions cannot be provided by cable, a qualified security officer will be sent to the Station or Base either from the appropriate regional group or Headquarters.
- E. Obtain appropriate increased guard coverage until the alarm is again operational.

~~SECRET~~

Page Denied

Next 10 Page(s) In Document Denied